Volume 16, Issue 04   Atari Online News, Etc.   January 24, 2014

Atari Online News, Etc.
A-ONE Online Magazine
Dana P. Jacobson, Publisher/Managing Editor
Joseph Mirando, Managing Editor
Rob Mahlert, Associate Editor

Atari Online News, Etc. Staff

Dana P. Jacobson -- Editor
Joe Mirando -- "People Are Talking"
Michael Burkley -- "Unabashed Atariophile"
Albert Dayes -- "CC: Classic Chips"
Rob Mahlert -- Web site
Thomas J. Andrews -- "Keeper of the Flame"

With Contributions by:

Fred Horvat

To subscribe to A-ONE, change e-mail addresses, or unsubscribe,
log on to our website at: www.atarinews.org
and click on "Subscriptions".
OR subscribe to A-ONE by sending a message to: dpj@atarinews.org
and your address will be added to the distribution list.
To unsubscribe from A-ONE, send the following: Unsubscribe A-ONE
Please make sure that you include the same address that you used to
subscribe from.

To download A-ONE, set your browser bookmarks to one of the
following sites:

http://people.delphiforums.com/dpj/a-one.htm
Now available:
http://www.atarinews.org

Visit the Atari Advantage Forum on Delphi!
http://forums.delphiforums.com/atari/

=~=~=~=

A-ONE #1604   01/24/14

~ ISPs, Common Carriers? ~ Broadband Speed Record ~ "Password" Not #1!

-* Judge Overturns Madden Ruling *-
-* Healthcare.gov’s Poor Security Test *-
-* China Censors May Have Caused Web Outage! *-

=~=~=~=

->From the Editor’s Keyboard   "Saying it like it is!"
""""""""""""""""""""""""""

Okay, so I may have caused a small furor last week; I received a few e-mails as a result of my comments. I was pleased at the comments and they were supportive in a variety of ways. People understand that it takes a lot of time and work to put this magazine together week after week; and we’ve been doing it for over 15 years now. People also understand (and have for many years now) that our original focus - to cover computer-related news - especially Atari-related in A-ONE’s original focal point - has changed over the years. Regarding Atari, there just isn’t any news that’s really relative to our computing "passion" of yesteryear. What’s it been, perhaps 20 years or so since Atari had any real relevance within the computing scene? In the world of technology, those were the dark ages!

I still fondly remember using all of my Atari systems, and the plethora of software that I used to enjoy using. I’m sure that we all do. I still have it all, but it’s all been put away in closets and stored in many boxes in the house. Yes, I’ve been using a Windows-based computer for many years ago. And, while it’s true that they don’t get the same type of use that I had with my Atari uses, a lot of that is because my needs andinterests have also changed over the years. I no longer spend a lot of time playing games, doing productivity or working with a publishing program. I still spend a lot of time online, but I really cannot do so [well] using my Atari systems. So, I moved on to systems that will allow me to better utilize my time - things change.

So, while I’ve been enjoying putting A-ONE together for all of these years, things continue to change. As I mentioned last week, when doing this magazine starts to become more work than enjoyment, it may perhaps be time to reevaluate. And, that’s what I’m in the process of doing. I do appreciate the continued support, and the occasional e-mails and article contributions - they mean a lot. I hope that continues for as long as A-ONE remains. I’ll keep you posted; we won’t just disappear one week and fade into oblivion without a whimper!

Until next time...

=~=~=~=

->In This Week’s Gaming Section - Nintendo Won Its First Console War 28 Years A

go!
""""""""""""""""""""""""""""""   Judge Overturns Ruling in Madden Football Cas
e!

=~=~=~=

->A-ONE’s Game Console Industry News   - The Latest Gaming News!
""""""""""""""""""""""""""""""""""""

Twenty-eight Years Ago This Month, Nintendo Won Its First Console War

Twenty-eight years ago this month, Atari took on Nintendo... and lost.

In January of 1986, Atari re-released the Atari 7800 - and promptly ran into the buzzsaw that was the Nintendo Entertainment System. Little remembered today, the event marked the end of Atari’s status as the dominant player in the home console market.

The home console business infamously crashed in 1983, but that didn’t keep companies like Atari from churning out new systems. First launched in 1984, the Atari 7800’s major selling points included backward compatibility with the Atari 2600 and an expansion slot that could house a High Score Cartridge. However, legal issues arising from the console’s development (see: it hadn’t fully paid the console’s designers yet) forced Atari to pull it from shelves soon after its arrival, leaving it to molder in warehouses for another two years.

Fast-forward to January 1986, just a few months after the initial release of the Nintendo Entertainment System. Unfortunately for the 7800, it seemed dated by comparison. The colors weren’t as vibrant, the music wasn’t as sharp, and the game library mainly consisted of retreads from the glory days of the Atari 2600. The NES was superior in pretty much every way, and it had one of console gaming’s first true killer apps: Super Mario Bros.

In addition to these shortcomings, the Atari 7800 was also one of the earliest victims of Nintendo’s licensing policies, which forbade developers from porting their games to other consoles. Thus, without a viable library or retail presence, it was quickly banished to the far corners of the marketplace, where it joined contemporaries like the Sega Master System. Today, it retains a small but fanatical homebrew community - not quite a new lease on life, but enough that is remembered.

As for Nintendo, it received its eventual comeuppance in 1995, when the same licensing practices that killed the Atari 7800 drove developers into the arms of Sony and the PlayStation. Ultimately, Nintendo’s desire to establish strict controls on development likely saved it from the sort of glut of awful titles that nearly killed the industry in the first place.

Judge Overturns Ruling in John Madden Football Designer’s Case

Despite winning his case against Electronic Arts back in July, John Madden Football designer Robin Antonick will not see his promised $11 million. The San Francisco Chronicles reports US district judge Charles Breyer has overturned that ruling.

Breyer said there was no clear evidence that Antonick’s work had been copied by EA without his permission. Breyer added that jurors in the original ruling weren’t shown Antonick’s game alongside EA’s subsequent efforts, as the law requires in copyright infringement disputes, and therefore were unable to make a proper evaluation. Antonick’s lawyer Robert Carey said they plan to appeal Breyer’s new ruling, of course, and added that evidence showed EA "used his source code without permission."

Antonick first filed suit against EA back in 2011. The original John Madden Football launched in 1988 on the C64, Apple 2 and on MS-DOS. The modern incarnation of the series is one of EA’s most successful franchises. Antonick is currently working on a basketball game called Grudge Match.

=~=~=~=

A-ONE’s Headline News
The Latest in Computer Technology News
Compiled by: Dana P. Jacobson

China Censors May Have Caused Huge Internet Outage

China’s Internet suffered a massive breakdown as traffic was routed to an overseas site linked to the banned religious group Falun Gong - a fiascoa cyber-monitoring group Wednesday blamed on the country’s own censors.

Web users in the country - which tightly restricts Internet access - had trouble accessing numerous sites for about an hour on Tuesday afternoon, said Greatfire.org, which tracks the vast Chinese online censorship apparatus known as the Great Firewall.

"We have conclusive evidence that this outage was caused by the Great Firewall," it said on its website, calling the incident "one of the largest Internet outages ever in China".

Internet users were sent to an IP address owned by US-based Dynamic Internet Technology, which runs a tool called FreeGate designed to bypass Chinese internet censors.

The IP address - 65.49.2.178 - is linked to dongtaiwang.com, a news portal run by Falun Gong members, Greatfire.org said.

The state news agency Xinhua raised the possibility of hacking, and the official China Internet Network Information Centre attributed the breakdown to a "root server for top-level domain names".

But Greatfire.org cast doubt on those claims, citing technical tests and saying such an act was "not enough to cause this outage".

Falun Gong is a Buddhist-inspired religious group that was banned in China in 1999 and branded an "evil cult".

Dynamic Internet Technology lists as clients on its website the Epoch Times - a publication linked to the spiritual movement - along with Human Rights in China and other groups.

China’s vast censorship apparatus proactively suppresses any information or websites online deemed sensitive, from popular sites such as Facebook and Twitter to a frequently updated list of search terms.

FBI Warns Retailers That Target Fiasco Could Happen to Them

Consumers who weathered the Target scare shouldn’t think they’re out of the woods yet.

The FBI is warning that more cyber attacks are likely after the agency discovered around 20 cases similar to the Target hacking fiasco that exposed millions of customers’ credit cards, Reuters reported.

The similar cases used the same kind of malicious software that infiltrated Target’s system to compromise 70 million customer accounts.

In a confidential report, the FBI warned retailers to beware the risks associated with "memory-parsing" malware that can breach such systems as cash registers and credit card machines.

"We believe POS malware crime will continue to grow over the near term, despite law enforcement and security firms’ actions to mitigate it," said the FBI report, seen by Reuters.

"The accessibility of the malware on underground forums, the affordability of the software and the huge potential profits to be made from retail POS systems in the United States make this type of financially motivated cyber crime attractive to a wide range of actors," the FBI said.

An FBI spokeswoman confirmed the report to Reuters.

The information stolen from Target customers included addresses, phone numbers and credit and debit card numbers.

Target has announced that it will offer one year of free credit card monitoring and identity theft protection to those who visited U.S. stores on Black Friday through when the breach was discovered.

A recent similar data breach was at luxury chain Neiman Marcus. The hacking took place from July 16 to Oct. 30 of last year, exposing 1.1 million customer cards.

The inventor of the malware used on Target is still in question. Some outlets earlier reported that the software was created by a 17-year-old Russian boy.

The Wall Street Journal reported on Thursday that the malware may be partly the work of Rinat Shabaev, a 23-year-old who lives in southern Russia.

Security researchers said that Shabaev offered to sell copies of a version of the software used in the Target breach for $2,000 each.

Gmail Was Down for Many Users Friday Afternoon

Productivity ground to a halt yet again as a brief outage at Google kept many users from being able to use Gmail on Friday afternoon.

The worst of the outage lasted for approximately 10 minutes, though services remained unstable for about an hour. But it was long enough to send Gmail s millions of users to Twitter to complain about not being able to check their e-mails.

Google said it s looking into why some user services were unstable or inaccessible for up to an hour.

Those trying to access their accounts were greeted with an error message from Google saying that the accounts were temporarily unavailable. The message also directed users to look at the company s Apps Status Dashboard for updates on the outage. The dashboard initially showed no disruptions for any Google services, but was later updated to show problems with Google Calendar, Google Talk, Google Drive, Google Groups and other services.

Some users on social media networks also reported that they were unable to open their Google+ accounts, even after mail had been restored.

In a statement, Google said that it is investigating reports of an issue with some Google services and will be posting updates to its Apps Status Dashboard. All services on the Google Dashboard were working as intended, at about 4 p.m. on Friday afternoon.

The company hasn t released official usage numbers for Gmail in over a year   the firm last touted 425 million in June 2012   but companies that partner with Gmail, such as Todoist, have said that Gmail now has over 500 million accounts.

The service has not had a major outage since 2009, when an issue with one of the company s servers caused communication problems for days. But hiccups with the system are not uncommon. Most recently, Gmail and Google Docs were both hit by a limited outage in April that left some users unable to access their messages, documents or Google chat for the better part of the morning.

Healthcare.gov’s Poor Security Diagnosis Shows Importance of Security Lifecycle

Four minutes   that is how long security researcher David Kennedy said it took him to expose a hole that could have allowed him to access information on 70,000 people courtesy of Healthcare.gov.

The security of the website has become a political battleground in the fight over Obamacare. But behind the politics, Kennedy told SecurityWeek, are serious security issues caused by a rushed development cycle.

"They didn t have enough time to formally develop the website and grow in a manner to be successful," said Kennedy, founder of TrustedSec. "When that happens, security is put in the back burner to making sure you can get the site out in time. To this date, they can t be doing any formal testing all around on the site. Maybe some here or there, but nothing that we would consider industry best practices."

While he declined to get into the specifics of what he did because the issue is still present, he described it as not so such much a hack but an abuse of the site’s legitimate functionality.

In testimony before Congress last week, Teresa Fryer, chief information officer of the Centers for Medicare and Medicare Services (CMS), testified that the site had passed a "security control assessment" in December and had "no open high findings." In his testimony however, Kennedy disagreed, claiming that only half of the 18 major issues he had previously told Congress about in November had been fixed.

"Vulnerabilities are a fact of life for any large scale service delivered via the Internet, and especially the web," Tim Erlin, director of IT risk and security strategy for Tripwire, opined in an interview with SecurityWeek. "The problem here is not that these vulnerabilities exist, but that there seems to be no defined process for addressing them, outside of political mudslinging and defensive posturing. Commercial vendors deal with this reality on a daily basis."

"People, both customers and researchers of varying affiliations, find vulnerabilities," he continued. "They are encouraged to report them to the affected vendor first, but some are disclosed publically with no vendor notification, or are discovered through their exploitation by criminals. The vendors establish a process for validating, responding and fixing these issues. This kind of a process is what s behind Microsoft s monthly release of security bulletins. A good process assesses risk, adjusts priorities appropriately and provides a framework for setting expectations and for public response."

"Instead of engaging in a PR war, Healthcare.gov should implement a constructive process for finding, prioritizing, and fixing the vulnerabilities in their service," he added.

Kennedy agreed, arguing that healthcare.gov is not a solitary case. On the contrary, this is a federal and statewide issue, he said.

"There needs to be a higher governance structure where all security reports in through the fed/state in order to ensure appropriate controls and functioning security programs," he said. "Specifically for Healthcare.gov, I m not sure how they can [improve security] at this point, they just booted the developers for the original site and moved to a new one. It s going to be a mess for awhile.

"I hope Accenture incorporates best practices and performs full security reviews," he added. "The word FISMA compliance is thrown around as being secure. FISMA is far from security and anything from being close to industry best practices or a successful security program."

Google Lays $2.7 Million on the Line for Pwnium Hacking Contest

Google yesterday said it would again host its Pwnium hacking contest at a Canadian security conference in March, putting $2.7 million at stake to draw out researchers who can hack its browser-based operating system, Chrome OS.

Dubbed Pwnium 4, the challenge will again pit researchers against Chrome OS, but this year will let them choose between Intel- or ARM-powered laptops. In 2013, hackers had to try to crack a Chromebook with an Intel processor.

Prizes of $110,000 and $150,000 will again be rewarded to individuals or teams who can hack the operating system, with the top dollar handed to those who deliver an exploit able to persistently compromise an HP or Acer Chromebook - in other words, hijack the device so that it remains under their control even after a reboot.

Google capped the total up for grabs at $2.71828 million, giving multiple researchers a chance at prize money. The "2.71828" comes from a mathematical constant that is the base of the natural logarithm.

Last year Google put $3.14159 million in the pot - another nod to mathematics, as those are the first six digits of the value of Pi - but paid out just $40,000 to a prolific hacker who goes by "Pinkie Pie," the contest’s sole participant, for what Google later called a partial exploit.

Google also said it would consider larger bonuses this year to researchers who demonstrated what it called a "particularly impressive or surprising exploit," such as one that could circumvent kASLR, (kernel Address Space Layout Randomization), a relatively new variant of the better-known ASLR anti-exploit technology used by Apple’s iOS and OS X, Microsoft’s Windows 8 and Chrome OS.

Even with bonuses in play, it’s unlikely that Google will end up spending anywhere close to $2.7 million this year.

To qualify for the prizes or bonuses, winners must provide functional exploit code and details on all the vulnerabilities put into play, as was the case last year.

Pwnium 4 will take place March 12 at CanSecWest, the Vancouver, British Columbia, security conference known for another hacking contest, Pwn2Own, which last year was co-sponsored by HP’s Zero Day Initiative (ZDI) bug bounty program and Google. HP has not yet announced the details of its 2014 challenge.

The official rules for Pwnium 4 can be found on Google’s Chromium Security page.

On Facebook, Clicking ’Like’ Can Help Scammers

It’s an image that tugs at the heartstrings. A smiling 7-year-old girl poses in her cheerleading uniform, circled by a ring of pompons, her bald head a telltale sign of her chemotherapy treatments.

The photo hit Facebook last year and popped up all over with messages of support. "Like" to show this little girl you care. "Share" to tell her she’s beautiful. Pray for her to beat cancer.

But here’s the truth. The photo was nearly six years old. And neither the girl, nor her parents - who never posted it to Facebook - had any idea it was being used that way.

Welcome to the world of Facebook "like farming."

Those waves of saccharin-sweet posts that sometimes fill your news feed may seem harmless. But all too often, they’re being used for nefarious purposes. At best, a complete stranger may be using the photos to stroke their own ego. At worst, experts say, scammers and spammers are using Facebook, often against the site’s rules, to make some easy cash.

And they’re wiling to play on the good intentions of Facebook users to do it.

"The average user doesn’t know any better," said Tim Senft, founder of Facecrooks.com, a website that monitors scams and other illegal or unethical behavior on Facebook. "I think their common sense tells them it’s not true, but in the back of their minds, they think ’What if it is true? What does it hurt if I press like?’ or whatever."

What does it hurt?

"I was first shocked," said Amanda Rieth of Northampton, Pennsylvania, whose daughter was the subject of that photo. "And then infuriated."

After being notified by a friend who recognized the girl in a Facebook post, Rieth tracked the image back to a link she’d posted to her Photobucket account in a community forum in 2009, two years after it was taken.

Her daughter, who was diagnosed with Stage IV neuroblastoma in early 2007, has been featured in local news segments for her fundraising efforts to fight cancer through Alex’s Lemonade Stand. But her mom said she was always part of the decision and was happy to help publicize the fight.

"This? This was entirely different and entirely out of our control," Rieth said. "That’s the most gut-wrenching part: the total lack of control."

Hurting the people featured in the posts, and their families, isn’t the only risk of sharing such content. Sometimes, a single click can help people who are up to no good.

Often, Senft said, Facebook pages are created with the sole purpose of spreading viral content that will get lots of likes and shares.

Once the page creators have piled up hundreds of thousands of likes and shares, they’ll strip the page and promote something else, like products that they get a commission for selling. Or, they may turn around and sell the page through black-market websites to someone who does the same.

It’s a way to trick Facebook’s algorithm, which is designed to give more value to popular pages than the ones, like scams and spam, that pop up overnight.

"The more likes and shares and comments and that sort of thing you have, the more likely it is to be seen by other people," Senft said. "If they’re looking to sell the page in a black-hat forum somewhere, that’s what the value of the page is."

It gets worse

Sometimes, the threat is more direct.

The "new" page may be used to spread malware - software that attacks the user’s computer - or for phishing, the act of trying to gather credit card numbers, passwords or other personal information through links to phony giveaways or contests.

Simply liking a post, or the page itself, can’t spread a virus or phish a user. But malicious Facebook apps can, as can external links that page owners may choose to share to their followers.

If the page owner has access to Facebook’s developer tools, they can collect data on the people who like the page. Personal information like gender, location and age can be used to target more personalized attacks.

The kind of posts used run a gamut from cute to tasteless, from manipulative to misleading.

Rieth said she still finds her daughter’s photo on Facebook from time to time, even though Facebook eventually deleted the original after she and others reported it.

On the most recent page she found, the picture appears in a feed alongside posts such as "Who loves French fries? Like & share if you do" and multiple images encouraging people to like and share if they love Jesus.

There’s an image of a premature baby, pictures of military troops cuddling puppies and an image of a young boy pouring water on a man’s cigarette with the text "Sorry papa ... I need you."

"It’s anything that’s going to kind of tug at the heartstrings: the sick kids, the animal abuse, acting like it’s some kind of pet shelter," Senft said. "That’s the bad part with the scammers. They hit people where they’re vulnerable, play on their emotions."

Because of Facebook’s sheer size, he said it sometimes takes lots of reports for the site to delete an offensive or misleading image, or shut down the page it came from. The best approach, Senft said, is to think before sharing.

"If it sounds too good to be true, don’t click on it," he said. "If it’s something that’s obviously geared toward tugging on the heartstrings, check it out first."

Facebook said it continues to work to make sure high-quality content surfaces for users and low-quality posts don’t. That includes trying to diminish the reach of posts that appear to be "like farming" attempts.

"People have told us they associate requests to like or share a post with lower quality content, and receiving that type of feedback helps us adjust our systems to get better at showing more high quality posts," a Facebook spokesperson said via e-mail.

"If you see a post that’s low quality and seems to be focused only on gaining traffic, hover over the top-right corner of the post and click the arrow to report it."

Facebook uses "automated and manual methods to swiftly remove links and pages that violate our policies," the spokesperson said. "We’re always making improvements to our detection and blocking systems to stay ahead of threats."

Today, Rieth’s daughter is 13 - an eighth-grader who has shown no signs of her cancer since September 2007.

But her mom compares that cheerleading photo to the mythical hydra, a monster with many heads that sprouts two more each time one is cut off. Based just on the images she’s found and reported, the photo has been liked and shared on Facebook hundreds of thousands of times.

A search Monday also found it popping up on Pinterest, as well as one site where it was wrongly used alongside a 2010 article about actor Jackie Chan helping a girl with leukemia find a bone-marrow donor.

"What makes me truly angry, though, is knowing that they’re using it as an insidious way to make money," Rieth said. "That’s not what her survival is about to us."

For this article, CNN sent a Facebook message to the owner of the last page where Rieth found the photo.

When asked whether he planned to sell his page, the owner replied with two words:

"How much?"

Make ISPs Into "Common Carriers," Says Former FCC Commissioner

It’s time for the Federal Communications Commission to correct its past mistakes and get tough on broadband providers, a retired FCC commissioner says.

Michael Copps, an FCC commissioner from 2001 to 2011 (and acting chairman for several months in 2009), is proof that not every former FCC member becomes a lobbyist for the industries the commission regulates. The only commission member to vote against allowing the Comcast/NBC Universal merger, Copps is now a self-described public interest advocate who leads the Media and Democracy Reform Initiative at Common Cause.

The commission can still put ISPs under its thumb, but it may not want to. On Wednesday, Copps wrote a blog post titled, "The Buck Stops At The FCC," calling upon the commission to "reclassify broadband as ’telecommunications’ under Title II of the Communications Act." The effect of that move would be to designate Internet service providers as "common carriers," making them subject to increased FCC regulation.

Such a move would bring fierce opposition from telecommunications companies and their friends in Congress. But the FCC’s previous failure to reclassify broadband blew up in its face when a court ruled that that the agency couldn’t impose anti-blocking and anti-discrimination regulations on ISPs because they aren’t classified as common carriers.

"The good news is that the solution is pretty simple," Copps wrote. "It doesn t require a new telecommunications statute replete with time-consuming years of legislative horse-trading and special interest lobbying. All it requires is an FCC big enough to own up to its previous mistakes and courageous enough to put our communications future back on track."

He continued:

> The DC Circuit Court of Appeals pointed the way out of the dilemma created when the Commission reclassified broadband as an information service over ten years ago. The Court held that the Commission has authority to make decisions on broadband and that these decisions are entitled to considerable deference by the judiciary. The FCC could have decided on a different path and still garnered court approval. Importantly, it can also change course if it justifies the reasons for the change.
>
> What the judges said last week was that the Commission justified its Open Internet rules the wrong way. Had the agency just kept treating advanced telecommunications as telecommunications, its Internet Freedom rules would have passed muster. But by calling broadband an information service, the FCC put it beyond the reach of Title II which applies to telecommunications. And Title II is where such things as consumer protections, privacy guarantees, public safety, and ubiquitous build-out requirements pertain. Who, other than the big companies trying to gain market power over broadband, would ever have argued that Congress intended broadband communications to be stripped of such elemental consumer and public interest protections?
>
> The time is now for the FCC to classify broadband as Title II. Without this step, we are playing fast-and-loose with the most opportunity-creating technology in all of communications history. Without this step, we are guaranteeing an Internet future of toll-booths, gatekeepers, and preferential carriage. Without this step, we stifle innovation, put consumers under the thumb of special interests, and pull the props from under the kind of rich civic dialogue that only open and non-discriminatory communications can provide.

Copps ended his post by encouraging readers to sign a Common Cause petition telling the FCC to reclassify broadband.

Netflix has warned that without net neutrality regulations, "a domestic ISP now can legally impede the video streams that members request from Netflix, degrading the experience we jointly provide."

Current FCC commissioners have given no indication that they would reclassify broadband as Copps suggests, but current Chairman Tom Wheeler said he views the recent court decision as an invitation for the FCC to act... in some undefined way. "The court invited the commission to act, and I intend to accept that invitation," Wheeler said last week. "Using our authority, we will readdress the concepts in the Open Internet Order, as the court invited, to encourage growth and innovation and enforce against abuse."

That could mean rewriting the Open Internet Order to put it on solid legal footing, but the changes probably wouldn’t impose anti-blocking and anti-discrimination rules that prevent ISPs from blocking services and charging content providers for access.

Facebook Fires Back at Princeton ’80 Percent’ Study

Watch out, Princeton University. According to Facebook’s data, you could also soon be a thing of the past.

The social network on Thursday hilariously fired back at a recent study from the Ivy League school, which claimed Facebook will undergo a rapid decline in the coming years, losing 80 percent of its peak user base between 2015 and 2017. In a tongue-in-cheek post Thursday, Facebook data scientists Mike Develin, Lada Adamic, and Sean Taylor used "the same robust methodology featured in the [Princeton] paper" to argue that the New Jersey school is, in fact, also at risk of dying off.

According to Facebook’s not so scientific research, Princeton will have only half its current enrollment by 2018, and by 2021 it will have no students at all.

"Based on our robust scientific analysis, future generations will only be able to imagine this now-rubble institution that once walked this earth," the researchers wrote.

The social network first examined Facebook Page "likes" for Princeton compared to Harvard and Yale, and discovered an "alarming trend." While page likes for Harvard and Yale ramped up significantly in recent years, Princeton suffered a massive drop in page likes in 2010, and has only slightly recovered in the years since.

"While we are concerned for Princeton University, we are even more concerned about the fate of the planet   Google Trends for ’air’ have also been declining steadily, and our projections show that by the year 2060 there will be no air left," they joked.
Advertisement

The social network kids, of course. "As data scientists, we wanted to give a fun reminder that not all research is created equal   and some methods of analysis lead to pretty crazy conclusions," the researchers wrote.

European Telecoms Break Broadband Speed Record

Two European telecommunications companies claimed this week that they achieved the fastest ever real-world fiber network transfer speed using commercial grade hardware.

According to a report released Tuesday, France’s Alcatel-Lucent and Britain’s BT achieved fiber speeds of 1.4 Terabytes per second. That’s roughly the equivalent of transmitting 44 HD films in a single second.

Researchers accomplished this quite spectacular feat by developing an "Alien Super Channel," which consists of seven 200 Gb/s channels bundled together for a combined capacity of 1.4 Tb/s. The trial test was conducted over an existing fiber link between the cities of London and Suffolk, England.

Perhaps the most intriguing part of the test was that it was merely an improvement in the efficiency of existing fiber networks not a radical redesign of the network infrastructure. By increasing the density of fiber channels, researchers achieved up to 42.5 percent greater transmission efficiency compared to standard networks.

This means future applications of the technology could reduce the cost of laying additional fiber cable a major obstacle to widespread adoption of consumer-grade gigabit broadband.

Fiber-optic networks are widely seen as the vessel that will get us to the super-fast broadband speeds needed to supply the ever-growing internet population’s ever-growing data demands. In the U.S., progress has been slow, with only a few scattered locations including a few spearheaded by Google currently enjoying access to fiber-optic speeds.

The problem is that major ISPs and cable providers, which often enjoy near total monopolies in the U.S., have little incentive to invest in the infrastructure fiber requires. As such, innovation in the sector is likely to remain in more competitive overseas markets, as demonstrated by this week’s record-breaking transmission.

Happy 30th Birthday to Apple s Macintosh Computer!

Today marks exactly 30 years ago that Steve Jobs took the stage in Cupertino, Calif., to introduce the world to Apple s Macintosh personal computer. The company had invested $80 million of research and development to reach that moment on Jan. 24, 1984, when the little beige computer personally uttered the above greeting to the world.

The Macintosh was priced at $2,495 at its launch and had a 3.5-inch floppy disk drive, black-and-white display and weighed 16 pounds (considered fairly portable at the time). The model shown off by Jobs that day was eventually renamed to the Macintosh 128K when Apple released an updated Macintosh 512K later that year (128 and 512 represented the amount of RAM the computers packed).

Apple’s Macintosh was the first mass-marketed PC to feature a graphical user interface and mouse controller. The new concept replaced the text-only, terminal OS style with an early version of the point-and-click software we now use on computers. Jobs would later famously accuse Microsoft co-founder Bill Gates of stealing the Macintosh software concept to create Windows.

Some recent eBay listings still have Macintosh 128K models selling for nearly $2,000, though considering inflation, that s still a darn good deal today.

Why Apple’s ’1984’ Commercial Is Still Talked About Today

On this day 30 years ago, Apple aired a commercial based on George Orwell’s dystopian novel "1984" that turned the advertising and computing world on their heads.

Long before the colorful, mysterious invitations to Apple s Cupertino, Calif., headquarters for product announcements, Apple mastered the art of creating buzz about its innovations.

Prime example: the ad it aired during the 1984 Super Bowl that aptly played off George Orwell s dystopian novel 1984." Using the simple themes of control versus freedom, and stagnation versus innovation, in a one-minute ad, Apple was able to spark viral curiosity just days before the release of its first Macintosh computer, and set a precedent-breaking tone that still prevails. The ad aired 30 years ago today.

The ad opens with a shot of a line of people in dark gray uniforms and shaved heads marching into an auditorium, where a talking head on a giant screen (a reference to Orwell s character Big Brother) spouts propaganda about being a garden of pure ideology ... secure from the pests of any contradictory force and one people with one will, one resolve, one course. This scene cuts back and forth with a scene of a woman in bright orange shorts and a white top holding a sledgehammer and sprinting toward the auditorium, guards in close pursuit. When she gets close to the screen, she winds up, launches her sledgehammer, and the impact creates a blinding explosion. Apple cuts to the tagline: "On January 24th, Apple Computer will introduce Macintosh. And you’ll see why 1984 won’t be like ’1984.’ "

The idea was that Macintosh would revolutionize computing and that the future of technology would bring freedom, rather than control. The message was effective   the ad launched Apple as a computing powerhouse, and made the Mac one of the best-selling computers of its time.

Before it aired at the Super Bowl, however, it nearly didn t make it to the screen. Apple had paid creative agency Chiat/Day $650,000 to create the ad as well as a second commercial. Steve Jobs was thrilled with the 1984 concept, but the board wasn t as impressed   according to Business Insider, Chiat/Day copywriter Steve Hayden says the board was struck silent after they were initially shown the ad, and were so unimpressed they told the ad agency to sell the two-minute block of advertising time Apple had bought during the Super Bowl. Apple ad account manager Fred Goldberg also tested the commercial with a leading market research firm for effectiveness, and it scored a 5 on a 43-point scale.

However, Chiat/Day executives were so enamored with the commercial, they intentionally dragged their feet, and were only able to sell half the airtime (also note that Mr. Goldberg decided to keep the market research numbers to himself). The commercial had to run.

Shooting the commercial also proved to be a challenge. The commercial was directed by Ridley Scott, who had directed "Blade Runner" and "Alien" in years previous. To give the ad the same gritty, futuristic feel while shooting in London, the creative team hired 300 locals as extras, many actual skinheads, who got a bit antsy after three days of filming.

"The last day they started throwing the rocks at each other," Goldberg told CNN. "The security company had police dogs there [to control them.]"

But the team behind the ad ultimately succeeded and the commercial was a rousing success for Apple. The ensuing conversation and ad replay on news programs and talk shows resulted in what Apple estimated as more than $150 million of free airtime.

The commercial is also credited with ushering in more than just a new era for Apple. Some say it brought about the modern era of Super Bowl advertising, in which the commercials are as much a spectator sport as the game.

"This commercial was classically disruptive," says Timothy de Waal Malefyt, a professor at Fordham University, to Business Insider. "This wasn t a machine where you were going to be kowtowed in the workplace, this was a machine for the young, innovative, entrepreneurial mind. It really inspires the creative individual to break free and start something different."

Chinese Internet Traffic Redirected to Small Wyoming House

In one of the more bizarre twists in recent Internet memory, much of the Internet traffic in China was redirected to a small, 1,700-square-foot house in Cheyenne, Wyo., on Tuesday.

A large portion of China s 500 million Internet users were unable to load websites ending in .com, .net or .org for nearly eight hours in most regions of China, according to Compuware, a Detroit-based technology company.

The China Internet Network Information Center, a state-run agency that deals with Internet affairs, said it had traced the problem to the country s domain name system. And one of China s biggest antivirus software vendors, Qihoo 360 Technology, said the problems affected roughly three-quarters of the country s domain name system servers.

Those servers, which act as a switchboard for Internet traffic behind China s Great Firewall, routed traffic from some of China s most popular sites, including Baidu and Sina, to a block of Internet addresses registered to Sophidea Incorporated, a mysterious company housed on a residential street in Cheyenne, Wyo.

A simple Google search reveals that the address on Thomes Avenue in Cheyenne is not a corporate headquarters, but a 1,700-square-foot brick house with a manicured lawn.

That address   which is home to some 2,000 companies on paper   was the subject of a lengthy 2011 Reuters investigation that found that among the entities registered to the address were a shell company controlled by a jailed former Ukraine prime minister; the owner of a company charged with helping online poker operators evade an Internet gambling ban; and one entity that was banned from government contracts after selling counterfeit truck parts to the Pentagon.

Wyoming Corporate Services, the registered agent for Sophidea Incorporated, according to Internet records, did not respond to requests for comment on Tuesday afternoon.

It was not immediately clear what caused the traffic shift Tuesday. One Chinese newspaper suspected a cyberattack. But by late Tuesday, some technologists had come to an alternate theory: a backfiring of China s own Internet censoring system.

Sophidea appears to be a service that redirects traffic from one address to another to mask a person s whereabouts   or to evade a firewall.

Some technologists surmised Tuesday that the disruption may have been caused by Chinese Internet censors who attempted to block traffic to Sophidea s websites but mistakenly redirected traffic to the service instead.

That theory was buttressed by the fact that a separate wave of Chinese Internet traffic Tuesday was simultaneously redirected to Internet addresses owned by Dynamic Internet Technology, a company that helps people evade China s Great Firewall, and is typically blocked in China.

Bill Xia, who created Dynamic Internet Technology in 2001, told The Wall Street Journal Tuesday that his company had nothing to do with the traffic shift and also suspected that the problem was the doing of China s own Internet censors.

The disruption mirrored a similar incident in 2002 when Chinese Internet users attempting to access Sina.com were redirected to a banned website belonging to followers of Falun Gong, a spiritual movement banned in China.

Password Is No Longer The Most Common Password

The news that password is no longer the most common password for users might seem like good news to IT managers. Maybe it s a sign that they re finally beginning to take security seriously? That they re finally devoted to protecting information?

Not so fast. A new study by Splash Data shows the new favorite password is 123456. It moved up from second place, switching spots with password.

Other than satisfying that old rule of strong passwords containing at least one number, that s not exactly a giant leap forward for security.

And the rest of the list is full of old chestnuts too, from iloveyou to qwerty to the somewhat pushy letmein.

Password problems abound

These annual studies of weak passwords might elicit a chuckle or two. But the temptation to believe a good password is enough protect you might be a last-generation security mindset.

Password crackers contain dictionaries of all the words in the dictionary, the Bible and pretty much any other source out there that users might draw on for something memorable.

But until biometric solutions evolve beyond the fingerprint sensor on an iPhone, you ll have to live with these imperfect protections.

7 ideas for stronger passwords

Here are some ideas to pass along to users:

Make them unique. A stolen password on one account can easily be used as a guess or jumping-off point for cracking passwords on other accounts.

Don t use words. Dictionaries can be guessed. Combining several words doesn t work either.

Invent acronyms. Take first letters from song lyrics, favorite poems, etc. and use them to invent a new word. If those phrases contain numbers or upper-case words, so much the better.

Never write them down. This may seem like a no-brainer, but take a walk around your office. We bet you ll find at least one sticky note on the side of a monitor or a drawer that lists user names and passwords. Leave a reminder sticky note behind.

Change defaults right away. If a website or account is given a default password, get rid of it ASAP. Replace it with one of your own.

Sharing is not caring. No one should ever share a password with another user. Doing so only makes it harder to police who is doing what on your networks and could lead to problems when users move on from your company.

Make a perfect password   then throw it out. Don t stick with the same password for too long. Make it good, secure and memorable. Then ditch it. The longer you stick with the same password, the better the chance it will be uncovered or compromised.

GIFYs Celebrate The Internet’s Favorite Time Waster

The Internet has provided countless hours of mindless, GIF-fueled fun, and these animated, Web-based images will now be honored with their very own online award ceremony.

This marks the first-ever awards celebrating the animated GIF as more than a simple time-waster, but "as a medium, social commentary, and art form."

Twelve categories from design and film to science and politics represent the best of the best of 2013, as nominated by a panel of 15 tech/entertainment editors, illustrators, writers, and other creative types from around the Internet.

Sponsored by advertising agency Crispin Porter + Bogusky (CP+B), The GIFYs provide five or six videos in each category, including the time-honored "cats" genre. Almost guaranteed to waste at least 45 minutes of your life, the awards include looping videos of sea otters, Oprah, Hillary Clinton, Breaking Bad, Mad Men, and a handful of other mesmerizing, and often hilarious, clips.

"Winners are immortalized on our website, finally giving GIFs their rightful glory," The GIFYs page said.

The site launched on Jan. 21, and voting remains open for a few more days.

The Graphics Interchange Format (GIF) launched in 1987, but caught on among Internet users, who can now post the animated videos on social corkboard Pinterest.

Despite their popularity, the debate over correct pronunciation GIF versus JIF rages on.

=~=~=~=

Opinions presented herein are those of the individual authors and do not necessarily reflect those of the staff, or of the publishers. All material herein is believed to be accurate at the time of publishing.